REMARKS

Claims 1-35, 69-79, 88, 89-91 are pending. Claims 1, 69, 88, and 89 are in independent form.

As a threshold matter, Applicant thanks the Examiner for considering the Amendment filed November 10, 2008 and for making the action mailed February 13, 2009 non-final.

Rejections under 35 U.S.C. § 103(a)

Claim 1 was rejected under 35 U.S.C. § 103(a) as obvious over U.S. Patent No. 6,477,651 to Teal et al. (hereinafter "Teal") and U.S. Patent No. 6,988,208 to Hrabik et al. (hereinafter "Hrabik").

As amended, claim 1 relates to a machine-implemented method for automatically identifying new signatures to use in identifying a previously unknown intrusive network attack. The method includes obtaining a collection of data items to be analyzed to identify the network attack, reducing said data items in said collection to reduce said data collection to a reduced data collection of reduced data items, wherein the reduced data items in the reduced data collection have a smaller size and a constant predetermined relation with data items in the data collection and at least some of the data items in the data collection that differ are reduced to the same reduced data item, analyzing a plurality of said reduced data items to detect

common elements in the plurality of said reduced data items, and sending the common content to one or more of a signature blocker and a signature manager. The analyzing identifies common content indicative of a previously unknown network attack. The data items are parts of messages that were sent over a data network.

The rejection of claim 1 is based on the contention that it would have been obvious for one of ordinary skill to have combined Teal and Hrabik to have arrived at the recited subject matter. In particular, the rejection is understood to contend that Neal's analysis of network data to identify known attacks is encompassed by the recited identification of common content to use in identifying an intrusive network attack. *See, e.g,. action mailed February 4, 2009*, para. 2.1, 2.2.

Although applicant believes that those of ordinary skill would not reasonably conflate the analysis of network data to identify known attacks with the identification of common content to use in identifying an intrusive network attack, claim 1 has been amended to clarify, e.g., that *new signatures* indicative of a *previously unknown* intrusive network attack are identified. Further, common content is sent to one or more of a signature blocker and a signature manager.

Since Teal does not provide many details as to how the signatures that are loaded into Teal's intrusion detection system are actually identified, there are fundamental differences between Teal's focus and the context of the recited subject matter. Further, there is no reason to believe that Teal would send the content from a known attack to either of a signature blocker and a signature manager.

Hrabik does nothing to remedy these deficiencies in Teal. In this regard, Hrabik describes a hierarchical system for preventing a network attack. *See, e.g., Hrabik*, col. 4, line 42-44. The hierarchical system includes a "master system 60" that is connected to a subsystem 50 of multiple devices. *See, e.g., Hrabik*, col. 6, line 56-60; FIG. 4.

In operation, "events" are collected from various devices of subsystem 50 and aggregated into an event log. *See, e.g., Hrabik*, col. 9, line 48-55. In Hrabik, "events" (or, alternatively, "security events") are constituents of a network attack such as, e.g., a buffer overflow. *See, e.g., Hrabik*, col. 8, line 43-58. Elements in subsystem 50 and master system 60 consolidate, classify, and correlate the events. *See, e.g., Hrabik*, col. 10, line 10-67.

The rejection of claim 1 points to the classification of events by Hrabik as allegedly constituting reducing data items to a reduced data collection, as recited. In particular, the rejection points to Hrabik description that a classification engine "will combine … similar messages from different sources, reducing the level of redundancy within the data" as allegedly reducing data items.

Applicant respectfully disagrees for several reasons. For example, there is no reason to believe that Hrabik's combination of similar messages from different sources will have a constant predetermined relation with data items in the data collection. Indeed, Hrabik's classification would appear to necessarily adapt to different circumstances, such as when different messages are collected. Thus, there is no constant predetermined relationship between the combined messages and the individual messages. Hrabik's combination of similar messages thus does not constitute reducing data items, as claimed.

Further, it would appear that one of ordinary skill would not analyze Hrabik's combinations of similar messages in order to detect common elements, as recited in claim 1. Indeed, since combining the similar messages would appear to inherently require that common elements be identified, a subsequent analysis to detect common elements would appear to be unnecessary.

Hrabik thus not only fails to describe or suggest the recited reducing of data items, one of ordinary skill would not replace the recited reducing of data items with Hrabik's combination of similar messages to arrive at the recited subject matter.

Accordingly, claim 1 is not obvious over Teal and Hrabik. Applicant respectfully requests that the rejections of claim 1 and the claims dependent therefrom be withdrawn.

Claim 69 was rejected under 35 U.S.C. § 103(a) as obvious over Teal, Hrabik, and U.S. Patent No. 7,089,592 to Adjaoute (hereinafter "Adjaoute").

As amended, claim 69 relates to a machine-implemented method for automatically identifying new signatures to use in identifying a previously unknown intrusive network attack. The method includes monitoring network content on a network and obtaining at least portions of the data on said network, data reducing said portions of the data using a data reduction function which reduces said portions of the data to reduced data portions in a repeatable manner such that each portion which has the same content is reduced to the same reduced data portion and at least some of the portions that differ are reduced to the same reduced data portion, analyzing said reduced data portions to find network content which repeats a specified number of times in order to establish said network content which repeats

said specified number of times as frequent content, identifying address information of said frequent content, identifying the frequent content as associated with the previously unknown network attack based on said identifying and determining, and sending the frequent content to one or more of a signature blocker and a signature manager

The address information includes at least one of source information or destination information that characterizes the respective of sources and/or destinations of said frequent content and determining if a number of sources and/or destinations of said frequent content is increasing.

The rejection of claim 69 once again states that claim 69 is "[r]ejected under the same rational as claim 1." *See Office action mailed August 11, 2008*, page 14, line 2. The rejection does not identify any content of Adjaoute that allegedly renders the recited subject matter obvious.

Since 35 U.S.C. § 132 and 37 C.F.R. § 1.104(2) both require that the reasons for any adverse action be stated in an Office action, the rejection is facially deficient and Applicant requests that it be withdrawn. Further, Applicant respectfully requests that the reasons for the rejection of any claim, including claims 69, 88, and 89, be set forth so that Applicant may judge the propriety of continuing prosecution.

Further, Applicant respectfully disagrees with the rejection on several additional bases. For example, claim 69 relates to the identification of new signatures to use in identifying a previously unknown intrusive network attack.

As discussed previously, Teal is primarily concerned with loading signatures into an intrusion detection system and does not provide many details as to how those signature are identified. Adjaoute describes a single and common software solution that consists of three main components and various sub-modules. *See, e.g., Amendment filed November 10, 2008.* However, none of these various sub models in Adjaoute identify new signatures to use in identifying a previously unknown intrusive network attack, much less by the recited method.

As for Hrabik, Applicant will proceed under the assumption that the rejection of claim 69 is made on the same basis as the rejection of claim 1 discussed above, namely, Hrabik's combination of similar messages allegedly constitutes reducing data portions.

However, even if this contention were taken as true, claim 69 would still not be obvious in light of Teal, Adjaoute, and Hrabik. In this regard, claim 69 recites that reduced data portions are analyzed to find network content which repeats a specified number of times. Applicant respectfully submits that since Hrabik's combinations of similar messages are already

combined, one of ordinary skill would not find it obvious to analyzes the combined messages to find combined messages which repeat a specified number of times.

One of ordinary skill would thus not replace the recited reducing of data items with Hrabik's combination of similar messages to arrive at the recited subject matter. Accordingly, claim 69 is not obvious over Teal, Adjaoute, and Hrabik. Applicant respectfully requests that the rejections of claim 69 and the claims dependent therefrom be withdrawn.

Claim 88 was rejected under 35 U.S.C. § 103(a) as obvious over Teal, Adjaoute, and Hrabik.

As amended, claim 88 relates to a machine-implemented method for automatically identifying new signatures to use in identifying a previously unknown intrusive network attack. The method includes obtaining a collection of data items to be analyzed to identify the previously unknown network attack, reducing said data items in said collection to reduce said data collection to a reduced data collection of reduced data items, analyzing a plurality of said reduced data items to determine frequently occurring sections of message information indicative of a network attack, carrying out an additional test on said frequently occurring sections of message information, and based

on the additional test, sending some of the frequently occurring sections to one or more of a signature blocker and a signature manager.

The reduced data items in the reduced data collection have a smaller size and a constant predetermined relation with data items in the data collection and at least some of the data items in the data collection that differ are reduced to the same reduced data item.

Carrying out the additional test includes maintaining a first list of unassigned addresses, forming a second list of source addresses that have sent to the unassigned addresses on said first list, and comparing a current source of a frequently occurring section to said second list. The unassigned addresses are maintained as reduced addresses that have a smaller size and a constant predetermined relation with the unassigned addresses and at least some of the unassigned addresses that differ are reduced to the same reduced address. The source addresses are maintained as reduced addresses that have a smaller size and a constant predetermined relation with the source addresses and at least some of the source addresses that differ are reduced to the same reduced address.

The rejection of claim 88 contends that it would have been obvious for one of ordinary skill to have combined Teal, Adjaoute, and Hrabik to have arrived at the recited subject matter.

Applicant respectfully disagrees for several reasons. For example, claim 88 relates to the identification of new signatures to use in identifying a previously unknown intrusive network attack.

As discussed previously, Teal is primarily concerned with loading signatures into an intrusion detection system and does not provide many details as to how those signature are identified. Adjaoute describes a single and common software solution that consists of three main components and various sub-modules. *See, e.g., Amendment filed November 10, 2008.* However, none of these various sub models in Adjaoute identify new signatures to use in identifying a previously unknown intrusive network attack, much less by the recited method.

As for Hrabik, Applicant will proceed under the assumption that the rejection of claim 88 is made on the same basis as the rejection of claim 1 discussed above, namely, Hrabik's combination of similar messages allegedly constitutes reduced data portions.

Applicant respectfully disagrees for several reasons. For example, claim 88 recites that the reduced data items in the reduced data collection have a smaller size and a constant predetermined relation with data items in the data collection. However, Hrabik's classification would appear to necessarily adapt to different circumstances, such as when different messages are collected. Thus, there is no constant predetermined relationship between the combined messages and the individual messages. Hrabik's combination of similar messages thus does not constitute reducing data items, as claimed.

However, even if this contention were taken as true, claim 88 would still not be obvious in light of Teal, Adjaoute, and Hrabik. In this regard, claim 88 recites that an additional test is carried out on said frequently occurring sections of message information. As part of this test, unassigned addresses are maintained in a first list as reduced addresses that have a smaller size and a constant predetermined relation with the unassigned addresses and at least some of the unassigned addresses that differ are reduced to the same reduced address. There is no reason to believe that addresses involved in Hrabik's combination of similar messages are somehow maintained in this manner.

Thus, even if Teal, Adjaoute, and Hrabik were combined, one of ordinary skill would not arrive at the recited subject matter. Accordingly, claim 88 is not obvious over Teal, Adjaoute, and Hrabik. Applicant respectfully requests that the rejections of claim 88 and the claims dependent therefrom be withdrawn.

Claim 89 was rejected under 35 U.S.C. § 103(a) as obvious over Teal, Adjaoute, and Hrabik.

Claim 89 relates to a machine-implemented method for automatically identifying new signatures to use in identifying a previously unknown intrusive network attack. The method includes obtaining a collection of data items to be analyzed to identify the network attack, reducing said data items in said collection to reduce said data collection to a reduced data collection of reduced data items, analyzing a plurality of said reduced data items to detect common elements, obtaining a second subset of the same network packet for subsequent analysis, and based on the subsequent analysis, sending some of the common content to one or more of a signature blocker and a signature manager. The data items comprise a first subset of a network packet including payload and header. The reduced data items in the reduced data collection have a smaller size and a constant predetermined relation with data items in the data collection

and at least some of the data items in the data collection that differ are reduced to the same reduced data item. The analyzing reviews for common content indicative of a network attack.

The rejection of claim 89 contends that it would have been obvious for one of ordinary skill to have combined Teal, Adjaoute, and Hrabik to have arrived at the recited subject matter.

Applicant respectfully disagrees for several reasons. For example, claim 89 relates to the identification of new signatures to use in identifying a previously unknown intrusive network attack.

As discussed previously, Teal is primarily concerned with loading signatures into an intrusion detection system and does not provide many details as to how those signature are identified. Adjaoute describes a single and common software solution that consists of three main components and various sub-modules. *See, e.g., Amendment filed November 10, 2008.* However, none of these various sub models in Adjaoute identify new signatures to use in identifying a previously unknown intrusive network attack, much less by the recited method.

As for Hrabik, Applicant will proceed under the assumption that the rejection of claim 89 is made on the same basis as the rejection of claim 1 discussed above, namely, Hrabik's combination of similar messages allegedly constitutes reduced data portions.

Applicant respectfully disagrees for several reasons. For example, claim 89 recites that the reduced data items in the reduced data collection have a smaller size and a constant predetermined relation with data items in the data collection. However, Hrabik's classification would appear to necessarily adapt to different circumstances, such as when different messages are collected. Thus, there is no constant predetermined relationship between the combined messages and the individual messages. Hrabik's combination of similar messages thus does not constitute reducing data items, as claimed.

However, even if this contention were taken as true, claim 89 would still not be obvious in light of Teal, Adjaoute, and Hrabik. In this regard, claim 89 recites that subset of the same network packet is obtained for subsequent analysis. Hrabik does not describe or suggest that the original data packets are even available to be obtained for subsequent analysis after combination.

Thus, even if Teal, Adjaoute, and Hrabik were combined, one of ordinary skill would not arrive at the recited subject matter. Accordingly, claim 89 is not obvious over Teal, Adjaoute, and Hrabik. Applicant respectfully requests that the rejections of claim 89 and the claims dependent therefrom be withdrawn.

It is believed that all of the pending claims have been addressed. However, the absence of a reply to a specific rejection, issue, or comment does not signify agreement with or concession of that rejection, issue, or comment. In addition, because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

Applicant asks that all claims be allowed. No fees are believed due at this time. Please apply any charges or credits, to deposit account 06-1050.

Respectfully submitted,

Date: April 9, 2009

/John F. Conroy, Reg. #45,485/
John F. Conroy
Reg. No. 45,485

Fish & Richardson P.C.
PTO Customer No. 20985
12390 El Camino Real
San Diego, California 92130
(858) 678-5070 telephone
(858) 678-5099 facsimile